2007/2008 : Report 8

OFFICE OF THE

Auditor General of British Columbia

Managing Access to the Corrections Case Management System

March 2008

2008-02669/

2007/2008 : Report 8

OFFICE OF THE

Auditor General of British Columbia

Managing Access to the Corrections Case Management System

March 2008

Library and Archives Canada Cataloguing in Publication Data

British Columbia. Office of the Auditor General.

Managing access to the corrections case management ystem

(Report ; 2007/2008: 8)

ISBN 978-0-7726-5964-4

1. Criminal registers - Access control - British Columbia - Evaluation. 2. Criminal registers - British Columbia - Data processing. 3. Public records - Access control - British Columbia - Evaluation. 4. Information storage and retrieval systems - Criminal justice, Administration of -- British Columbia. 5. CORNET (Computer file). I. Title. II. Series: British Columbia. Office of the Auditor General. Report ; 2007/2008: 8.

KEB591.B74 2008 353.4'238709711 C2008-960071-1

KF9751.B74 2008

OFFICE OF THE
Auditor General
of British Columbia

LOCATION:
8 Bastion Square
Victoria, British Columbia
V8V 1X4

OFFICE HOURS:
Monday to Friday
8:30 a.m. – 4:30 p.m.

TELEPHONE:
250 387-6803
Toll free through Enquiry BC at: 1 800 663-7867
In Vancouver dial 660-2421

FAX: 250 387-1230

E-MAIL: bcauditor@bcauditor.com

WEBSITE:
This report and others are available at our Website, which also contains further information about the Office: www.bcauditor.com

REPRODUCING:
Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our Office with authorship when any information, results or recommendations are used.

OFFICE OF THE
Auditor General
of British Columbia

8 Bastion Square
Victoria, British Columbia
Canada V8V 1X4
Telephone: 250 387-6803
Facsimile: 250 387-1230
Website: http://bcauditor.com

The Honourable Bill Barisoff
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Sir:

I have the honour to transmit herewith to the Legislative Assembly of British Columbia my 2007/2008 Report 8: Managing Access to the Corrections Case Management System.

John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
March 2008

copy: Mr. E. George MacMinn, Q.C.
Clerk of the Legislative Assembly

Table of Contents

Auditor General's Overview 1

Executive Summary 3

- Overall Conclusion 5
- Key Findings 6
- Key Recommendations 8
- Response by Government 11

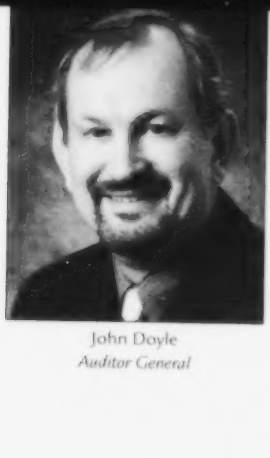
Detailed Report 15

- Background 17
- Audit Purpose and Scope 22
- Audit Approach 22
- Logical Access Security 23
- Organization-wide IT Security 36
- Patch Maintenance and Backup 36

Appendices 39

- A Office of the Auditor General Reports Issued Fiscal 2007/2008 41

Auditor General's Comments



John Doyle
Auditor General

Security vulnerabilit
by those who are just c
Such threats can come
from trusted insiders.

To guard against inf
designed, implemented
security should never b
security department. Ra
achieved through the co
measures, attuned man
activities, and system u
responsibilities.

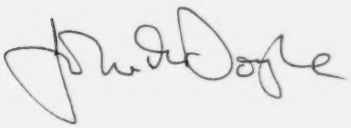
The corrections case
several thousand provin
users varying levels of a
confidential information
this information could b
access to this informatio

Our audit of the cont
the CORNET system fou
diligent in ensuring that
We found more weakne
the information could be

This audit is one of th
examinations we have d
I believe it is important
planned and implement
During my mandate, I in
these examinations. I am
quality of data in these s
integrating systems and

Auditor General's Overview

I would like to thank the staff in the Ministries of Attorney General, Public Safety and Solicitor General, Children and Family Development, and Labour and Citizens' Services for the cooperation and assistance they provided to my staff during our work on this audit.



John Doyle, MBA, CA
Auditor General of British Columbia

Victoria, British Columbia
March 2008

Audit Team

Bill Gilhooly, Assistant Auditor General

Pam Hamilton, IT Audit Specialist

Ada Chiang, IT Audit Specialist

Executive Summary

The public expects government to properly manage access to confidential information, especially if disclosure could possibly threaten the health and safety of citizens. Managing user access to information and applications is like managing access to a building. Each person granted access will be given keys that let them into rooms where they need to go to do their jobs. Some will have limited access, with keys to only a few doors. Others, usually very few, will have access to virtually all the doors.

CORNET is the corrections case management system, used for the administration of offender sentences and supervising offenders according to terms set in the court system. It contains large amounts of sensitive and confidential information about adult and youth offenders including offences committed, personal information, movements, court documents, sentence calculations, risk needs assessments, security classifications and victim information.

If system access is not properly configured, granted and maintained, or security measures are not in place to prevent break-ins, unauthorized viewing or changing of data could result. This in turn could lead to loss of privacy, injury or loss of life, breach of public trust, or contravention of the law and regulations for youth protection.

In our audit, we examined in detail who is granted access to this data, and how well it is being managed. For example, we looked at areas such as sentence management (excluding how release dates are calculated) in terms of who was able to change sentences and whether it was appropriate for them to have this access.

Overall Conclusion

Managing database access in the justice environment is challenging. On the one hand, those that manage user access need to ensure that it is set up so that key information is available to the right staff, at the right time. If it is too restrictive, the work environment becomes inefficient, or worse, personal safety could be put in jeopardy. On the other hand, they are responsible to ensure that access meets all legal requirements. This balancing act is juxtaposed with the need to be vigilant in protecting the information from those with criminal intent.

Executive Summary

Overall, we found that government has adequate access controls for most of the regular users that access CORNET. We also found that, although the controls that prevent or detect unauthorized internet access through the firewall were generally adequate, there was excessive entry to the database from internal users.

Our audit identified significant database access issues that could allow users to bypass all information security controls and restrictions. Government acted quickly when we brought these issues to their attention and dealt with them early on in our audit.

We also noted that processes were not strong over adjusting ongoing application access, based on changes in user employment status. These problems were also discussed with government and corrected quickly.

We have identified a number of key findings, and have key recommendations in most of the audit areas we examined.

Key Findings

- Appropriate controls are in place to ensure that only authorized users of the CORNET application are issued userids and granted access to the system. The procedures used to issue initial passwords and password resets provide adequate protection to prevent the risk of compromised passwords.
- Application controls are properly set up according to user job positions and, except for a relatively small percentage of incorrect accesses, are appropriately assigned to users according to their job positions and locations.
- Although most users are given correct access when first assigned it, access levels are not always updated in a timely way when users retire, resign, or are terminated, laid off or transferred. This results in a number of users retaining access when they no longer require it.
- The CORNET application properly protects sealed and youth data when entry is via the application. However, in some cases, incorrect access assignments resulted in inappropriate access to such data.
- Authorized system users are not properly restricted at the database level from gaining unauthorized access, potentially giving many users access to view, change or download data if they entered directly to the database. As well, there is no monitoring in place to see if this activity is occurring.

- Key staff who maintain the database need full access to do their work. They therefore have been given direct access to data in the database, including the ability to view and alter data directly and to overwrite the audit trail. Missing, however, is sufficient monitoring to detect unauthorized changes.
- The Oracle userid in UNIX is powerful, allowing full access to the CORNET database without needing to have a separate database userid and password. The Oracle userid is shared by several IT support staff. This creates a risk that if it was compromised or used inappropriately, identifying who was using it would be difficult. In addition, the password is set to the same value on all Ministry of Attorney General database servers. This creates a risk that if the password was compromised in any of the environments, unauthorized access to all of the ministry's databases, not just the CORNET application and database, could be possible.
- Firewalls are among the tools used to protect access to IT environments from entry outside the permitted network.[1] Although firewalls protect the CORNET environment from Internet traffic, the firewall settings allow excessive access to the database servers by users entering the system through government's SPAN/BC network.
- Most large IT vendors provide updated versions of their products that are meant to improve their usefulness, fix known problems, or handle new or emerging security threats. This updating process (often called "patching") is required to ensure systems are protected from the latest known threats. For the CORNET environment, the patching processes are not being done regularly, leaving the systems at risk of being compromised.
- The Ministry of Attorney General security group sets the security policy of the Justice Sector, but the group has had limited input to the security-related decisions in the CORNET system. Many security-setting decisions are made and implemented by Ministry of Attorney General IT support staff without any involvement or advice from the security group. The oversight of security policy and implementation appears to lack the integrated approach necessary for building a robust security environment.

[1] A firewall is a dedicated appliance, or software running on another computer, that inspects network traffic passing through it and denies or permits passage based on a set of rules.

Key Recommendations

We identified 92 recommendations as a result of our audit. These recommendations were included in a management report sent to the Ministry of Attorney General and the Ministry of Public Safety and Solicitor General in March 2008. We have not published all the detail for the findings and recommendations from this report, in part to avoid introducing any security risks. Exhibit 1 lists the number of recommendations we made by audit area and the number of summarized key recommendations in the executive summary.

These nine key recommendations address the key findings:

1. A process should be implemented for promptly informing key staff when user access needs to be modified because an employee's status has changed.
2. Exception reporting and regular monitoring should be conducted to identify and remedy incorrect access.
3. The database access levels should be corrected and regular monitoring conducted to ensure that access remains properly set and that all entries made directly to the database are detected.
4. Strategies, including effective monitoring, should be adopted to address the risk of users having full access.
5. Remove the ability to overwrite the audit trail from all users accessing the database directly.
6. The Oracle userid should be locked and only authorized support staff allowed to access it through their own userids.
7. Firewall settings should be reviewed and any excessive access removed.
8. A patching strategy should be adopted and implemented to address security related vulnerabilities.
9. A strategy should be developed to ensure the adherence of security policies in the implementation of security settings and processes.

Exhibit 1:

Key Areas Audited and Number of Recommendations

Audit Scope Area	Number of Management Report Recommendations	Number of Key Recommendations Summarized into Executive Summary
A. Logical access security		
1. Account access and maintenance	5	1
2. Login and authentication	9	4
3. Userid control settings	2	none
4. Monitoring of login access	none	none
5. Logical access to the database via database privileges	20	7
6. Logical access directly to the database via tools, utilities or other interfaces	11	4
7. Auditing at the database level	7	2
8. Logical access to the data via the application	11	5
9. Auditing at the application level	none	none
10. Logical access to the data via the host operating system	12	3
11. Logical access to the database via the network	13	6
Subtotal	90	32
B. Organization-wide IT security	1	1
C. Patch maintenance and back-up	1	1
Total recommendations	**92**	**34**

Response by Government

Response by Government

This combined response is provided on behalf of the Information Technology Services Division (ITSD), Ministry of Attorney General, the Corrections Branch, Ministry of Public Safety Solicitor General and Youth Justice Services, Ministry of Children and Family Development.

We would like to express our appreciation to the audit team for its thorough examination of Managing Access to the Corrections Case Management System (CORNET). We were encouraged by the confirmation that our systems were well protected from inappropriate external access and staff access was appropriate in most instances. The audit provided specific intelligence and effective insight to improve our access controls and security.

Our staff worked closely with the audit team throughout the review and took immediate action as required to address concerns identified during the examination. The audit also identified some processes and practices which will require longer term strategies to ameliorate. The result has already improved the security of the application and access to the database and we are committed to addressing the findings and recommendations contained in the audit.

Effective management of offenders requires timely and comprehensive access to sensitive information to protect the public, vulnerable persons and offenders. It is imperative for staff in a correctional centre on a 24 x 7 basis to have access to specific data concerning the risk posed by a new admission in order to protect staff and other offenders. This need has to be balanced against the requirement for strong system security and access.

ITSD and associated justice partners have adopted a strategy of "defense in depth" to strengthen the security of justice information and infrastructure. The following projects are completed or underway and will directly enhance our ability to address the findings and recommendations.

- The upgrade to Oracle 10G, including current security patches has been completed.
- The Data Centre recently moved all justice databases to the new high security zone and restricted direct access to the CORNET database.
- All security zone firewalls were replaced in 2007 and a formal review process is in place to validate rules.

- New tools designed to automatically scan and report on potential operating systems issues across all security zones will be online May 2008.
- By August 2008 the security department will be included in the System Development Life Cycle (SDLC) for new or enhanced applications. New applications will be scanned for security flaws prior to deployment in the production environment.
- External access to the security zones will require all users to have two factor authentication by March 2009—this encrypted secure enterprise solution will only allow access to applications and databases to certified users.
- Internal access to all justice applications will require two factor authentications by 2011.

To address the findings and recommendations contained in the audit the Ministries are committed to the following actions and strategies:

- All staff have been reviewed for appropriate access to the application and database, including their locations and roles. New directives have been put in place and policies and procedures are underway to ensure quarterly reviews will confirm the decommissioning of dormant or inactive accounts.
- Effective April 2008 technical staff with appropriate direct access to the database will have unique userids, additionally audit logs will be modified to enable long term monitoring and investigations of activity.
- The security department will coordinate with technical staff to review and recommend an action plan for all system patches to ensure security is enhanced without compromising the business applications.

Detail

Background

The Corrections Network System (CORNET), implemented on February 7, 2005, is an automated offender information and case management system for both adult and youth offenders in provincial corrections programs.[2] The system contains information on offenders who are supervised in custody and in the community or assessed for court purposes.

The CORNET system enhances operational workflow through built-in capabilities such as:

- admission of an offender after sentencing from courts;
- recording of entries to keep track of an offender's activity while in custody or in the community;
- sentence calculation to determine release date;
- scheduling of an offender's transfer between institutions, community centres or courts to manage the offender's movement; and
- program referral to support an offender's reintegration into the community.

CORNET is used primarily by institutional and community corrections officers for the management and supervision of both adult and young offenders. The data stored in CORNET includes information for about 400,000 current and inactive offenders, such as an offender's history, types of offences committed and the risks he or she poses. Currently in British Columbia, there are approximately 2,900 adult offenders in custody (either in remand or sentenced) and approximately 24,000 offenders in the community (either on bail or probation).

CORNET is connected to the JUSTIN[3] database, linking information on offenders in custody and in the community with court documents, events and reports in JUSTIN. The connection allows the staff responsible for offender supervision

---

2 The Corrections Branch of the Ministry of Public Safety and Solicitor General is responsible for administering the province's correctional system and programs for adult offenders. The Youth Justice Branch of the Ministry of Children and Family Development is responsible for administering custody and community programs for youth offenders.

3 JUSTIN is a single integrated database comprising almost every aspect of a criminal case, including police reports to Crown counsel, Crown counsel's case assessment and approval, victim and witness notification, court scheduling, results recording, document production, and judicial trial scheduling.

(Source: Ministry of Attorney General website at www.ag.gov.bc.ca.)

to receive electronic notifications and alerts in real-time concerning new court orders, scheduled appearance dates and the arrival of new offenders resulting from court decisions. As well, many administrative procedures are automated, including sentence calculation and the sealing of youth records as required by law.

There are about 4,000 CORNET users, of which about 3,300 (87%) are government employees from three ministries: Public Safety and Solicitor General, Children and Family Development, and Attorney General. All of these users have varying levels of access, from data viewing only to data entry and edit. Some users are given full access to the entire database. Others are limited to just viewing certain offenders' information or certain types of information. Youth records are protected and are only accessible under restricted conditions.

As part of an integrated justice information initiative, information on offenders is shared with several external justice and correctional authorities, including federal correctional officials, the provincial judiciary, Crown counsels and sheriffs, and local police forces in British Columbia. Agreements are in place with all external user groups accessing CORNET. These agreements cover the purpose for and extent of access privileges. At the time of our audit, 15 electronic access agreements were in place, allowing about 700 users from various external authorities to access CORNET.

Why are we looking at this area?

The CORNET system contains large amounts of sensitive and confidential information about adult and youth offenders including offenses committed, personal information, movements, court documents, sentence calculations, risk needs assessments, security classifications and victim information. The data provides valuable information to decision-makers, but in the wrong hands it could have detrimental consequences to public safety.

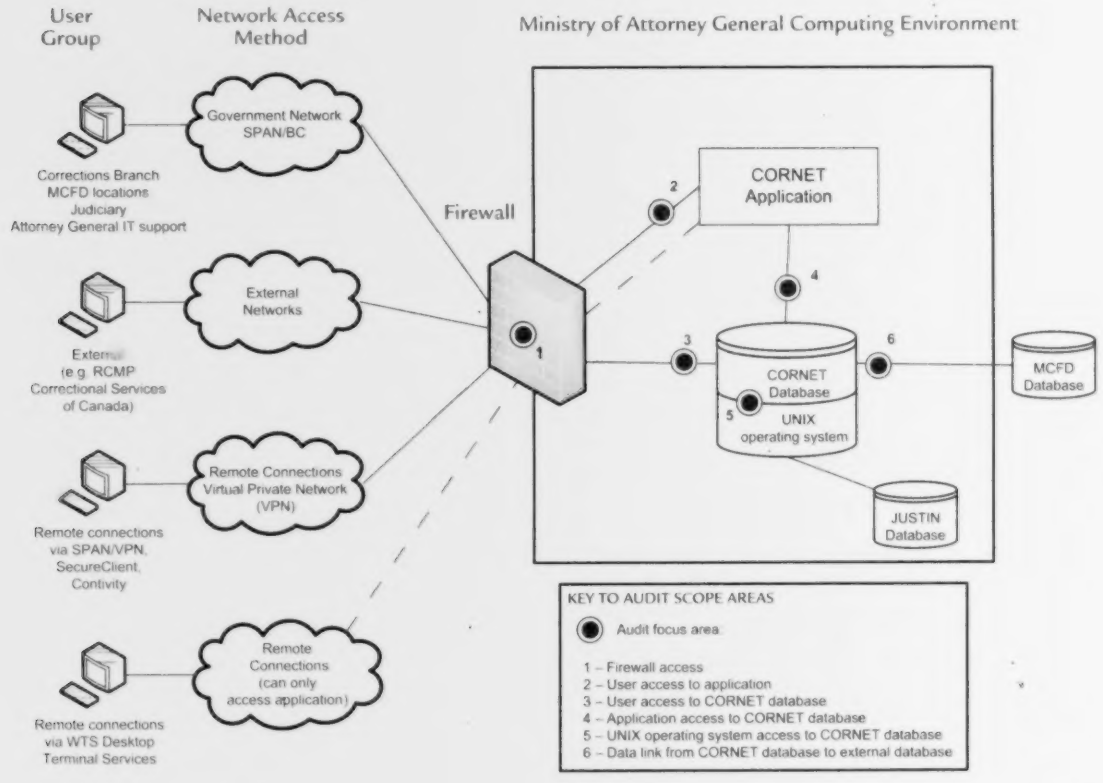
If system access is not properly configured, granted and maintained, or security measures are not in place to prevent break-ins, unauthorized viewing or changing of data could result. This in turn could lead to loss of privacy, injury or loss of life, breach of public trust, or contravention of the law and regulations for youth protection.

The computing environment

The CORNET application runs on a Solaris (a version of UNIX) operating system, using an Oracle database. The ORACLE database management system is designed to promote data consistency and integrity. The production system is located in the Ministry of Attorney General's computing facility in Victoria. This computing environment, and our audit scope areas, is shown in Exhibit 2.

Exhibit 2:

A simplified view of the CORNET computing environment and our audit scope areas



Source: Compiled by the Office of the Auditor General

Workplace Technology Services, a business unit of the Ministry of Labour and Citizens' Services, is responsible for managing the infrastructure required for network connectivity and for maintaining and operating the UNIX operating environment.

The Ministry of Attorney General provides full system support for the CORNET database, including security and maintenance, and shares the responsibility of application support and user access with the Ministry of Public Safety and Solicitor General.

The Corrections Branch and Ministry of Children and Family Development are co-owners of the CORNET System. The data relating to adults is owned by the Corrections Branch, and the data on young offenders is owned by Children and Family Development. Both ministries are responsible for the administration policy and procedures used by staff in carrying out their correctional duties, such as entering log entries, assessing risks, and calculating sentences.

Most users access the CORNET application from their workstations in a multi-step process. First, they log into their workstations and local network using their government userid and password. Then they log into the CORNET applications with their CORNET userid and password. Most users are connected to the application through a firewall over government's main network, called SPAN/BC, either from their local networks, or using other connectivity methods such as SPAN/VPN, SecureClient, Contivity or DTS.

Records in CORNET are typically created by correctional or probation officers, and court documents are brought in by way of an automated electronic interface with the JUSTIN database. CORNET accommodates electronic files from a variety of applications, and allows external data and images to be attached to offender files. Conversely, the system also has links to other ministries, allowing all or portions of the CORNET data to be copied to their databases.

What are the risks?

Ensuring a system's security means protecting its components from unauthorized access. The secure system depends on having appropriate controls over all components of the computing environment — the operating system, database and application — to prevent improper access to use, alter, destroy or disclose information.

For example, the operating system on which the Oracle database resides must be well protected. An insecurely configured operating system can put the entire database at risk. Anyone gaining access to the operating system could possibly gain full access to the database, and the opportunity to view or change all data. Weaknesses in the other parts of the environment, particularly database security, could compromise the security implemented at the application level.

For these reasons, strong access control to the computing environment is imperative. Access to systems should be provided on a need-to-know basis only, to limit potential abuse or misuse.

For this audit, we considered the following key risk areas for evaluation:

1. The risk that users could be granted access beyond what they require to perform their day-to-day duties. This could result in inappropriate access to sensitive or confidential information.
2. The risk that access to the system is not kept up to date, allowing unauthorized viewing or changing of data.
3. The risk that inadequate monitoring of the activities of staff with potential for unlimited access could allow fraudulent activity to go undetected or prevent later follow-up.
4. The risk that access to programs and highly sensitive data, specifically youth and sealed data, may not be restricted or monitored.
5. The risk that Oracle-based security and controls may not be adequately defined, resulting in a system that is less secure than it should be.

6. The risk that the operating system controls are not adequately managed to prevent unauthorized and undetected access to the CORNET database.
7. The risk that firewall controls do not properly protect the CORNET environment.
8. The risk that systems are not properly patched to address known vulnerabilities.

These key risks were considered in establishing the audit scope and identification of key control objectives and related procedures.

Audit Purpose and Scope

Our objective in examining the CORNET system was to assess whether adequate controls were in place to protect against unauthorized access to the information stored in the system.

The audit focused on controls relevant to accessing data through all entry points to the CORNET system: the Solaris (UNIX) operating system, the Oracle database and the CORNET application. These controls must operate effectively to ensure only authorized users can access the system in accordance with their business needs. The audit did not test for misuse of system information by users who have the authority and privilege to view that information.

Our examination addressed the following control objectives:

- Logical access to the UNIX operating system, Oracle database and CORNET application is properly controlled.
- Users are authorized and authenticated before gaining access to data.
- Appropriate measures have been taken to limit the exposure of unauthorized access.
- There are effective organizational level security structures and processes in place that help ensure a more secure system.

Audit Approach

Our audit was based on criteria set out in the *Information Technology Control Guidelines* issued by the Canadian Institute of Chartered Accountants. We used the standard control objectives provided in these guidelines to assess the design and the effectiveness of the IT controls in place.

We conducted the audit in accordance with assurance standards recommended by the Canadian Institute of Chartered Accountants. Accordingly, it included tests and other procedures we consider necessary to obtain sufficient and appropriate evidence to support our conclusions.

During our audit, we worked with staff from the Ministry of Attorney General, the Ministry of Public Safety and Solicitor General, the Ministry of Children and Family Development, and the Workplace Technology Services group of the Ministry of Labour and Citizens' Services.

Our audit included obtaining access to a complete snapshot of the database at a certain point in time, interviewing staff, examining user and system accesses in the CORNET database, verifying business processes outside of the system, and analyzing such controls as audit trails, firewalls and the host operating system.

We carried out the audit from June 2007 to January 2008.

Logical Access Security

In this section of the audit, we report on our assessment of controls we expected to find in place to ensure that access to the CORNET system and information is properly controlled. We examined 13 separate control areas, and have included our key findings and key recommendations.

A1. Account access and maintenance

How users are validated and granted access through userids and passwords is critical to ensuring adequate control. Equally important is the process of how these access rights are managed over time to ensure that control is adequately maintained. The Ministry of Attorney General is responsible for managing and maintaining access for database users. The Ministry of Public Safety and Solicitor General is responsible for assigning and managing application access.

Since some users may change job positions or employment status over time, their access rights may also need to change. When access is no longer needed, it should be removed immediately. For this to occur, key ministry staff must be notified promptly. This also means that users' supervisory staff must be aware of, and follow, processes

in place for ensuring timely notification of employment status changes. If the process breaks down, data security and integrity may be at risk, since access could be open to a large number of users who should no longer be authorized to access data and programs.

In this section, we looked at the controls in place to ensure that:

- procedures are adequate for setting up new users by authorized staff;
- user access was appropriately disabled or removed when changes in employment status occurred; and
- processes to obtain information on changes in user status and job function are in place.

Key Findings

- Proper controls are in place to ensure that only authorized users are issued userids and granted access to the system.
- User access is not always disabled or deleted promptly. Ongoing maintenance to adjust for changes in user status due to extended leaves, retirements and voluntary terminations was an issue because no standard process was being followed for notifying key people to make the necessary adjustments. As a result, a number of users still had access when they no longer required it.

We made five detailed recommendations in this area to improve controls over setting up and maintaining accounts access.

A2. Login and authentication

As is common in many systems, logical access to CORNET is controlled through userids and passwords. All passwords must remain protected to reduce the risk of unauthorized access to confidential information. Common control techniques are used, such as:

- requiring users to regularly change their passwords;
- using system-based rules to make passwords difficult to guess;
- requiring IT support staff to use different passwords in the production environment than in non-production areas such as the testing environment;

- requiring those with powerful access rights (such as system administrators) to set new password values to unique unknown strings; and
- changing or removing default passwords.

The effective use of these types of methods helps achieve system security by reducing the risk of unauthorized users accessing the system.

The ability of users to see or do anything in the system once they have logged in is also controlled by the access they have been given. The access that is granted to them at the database level must also be properly set to prevent data being inappropriately viewed or changed.

In this section, we looked at the controls in place to ensure that:

- access to userids and passwords in the database is appropriately controlled;
- appropriate controls exist over:
  - issuing, resetting, and changing passwords;
  - system-supplied default user accounts and passwords;
- passwords used in production by IT support staff are properly secured; and
- access issued to users at the database level is properly restricted.

Key Findings

- Procedures for issuing and resetting user passwords is adequate and the functionality allowing this to be done is appropriately restricted to authorized staff. Password resets and unlocks are done only if the system administrators have the right comfort level over the identity of the user calling in to have access reset.
- All users are required to change their passwords regularly. However, the same requirement is not in affect for IT support staff—individuals with very powerful access rights.
- Two IT support userids, with significant access rights, have the same password in production and non-production environments. This raises the risk that if the password was compromised in any of the environments, the production environment could be at risk.

- Database role access is improperly set up. This has made it possible for many users over the last several years to gain full access to all CORNET data, including youth and sealed data. To gain full access, these users would have to enter through the database not through the application. Although the majority would not know this capability existed, awareness of it could allow them access to change, view or download all the data in the database.

We made nine detailed recommendations in this area to improve controls over login processes and authentications.

A3. Userid control settings

The use of passwords does not guarantee a secure system. There are often inherent risks in user-defined passwords, including being easy to guess (e.g., family names, too few characters). To tighten password security, many systems today, including CORNET, have system-based controls that ensure users create and use passwords that are much more difficult to guess. For example, passwords with minimum lengths and that combine upper- and lowercase letters and numbers make it much more difficult to compromise passwords.

System settings can also used to automatically disable userids not used for certain lengths of time (e.g., 90 days), which may indicate users with changed positions or employment status. Logged-in users may also be disconnected if there is no workstation activity for a certain amount of time (e.g., one hour). These controls set up over userid settings should be in accordance with organizational policy and risk tolerance levels.

In this section, we looked at the controls in place to ensure that:

- security control settings (such as password strength, expiry and length; and sign-on time and timeout/background disconnect intervals) are set appropriately and are in line with government policy;
- parameters are appropriately set to control userid capabilities at the database system level, such as by limiting connection and periods of inactivity; and
- userid accounts are automatically disabled if not used for an extended period of time.

Key Findings

- Password control system settings (e.g., password strength, expiry and length) are set appropriately and are in line with government policy for all users. The exception is a few IT support users who can enter directly through the database.
- As a precaution, users who have not logged into the system for an extended period of time should have their userid disabled, as they may have had a change in employment status. Appropriately, the system automatically detects inactivity and disables the userid if it has not been logged into for 90 days.

We made two detailed recommendations in this area to improve userid control settings.

A4. Monitoring of login access

One way that someone might attempt to gain unauthorized access to systems is to try to log in with a valid userid and then repeatedly enter passwords until the one is recognized by the system. This can be done manually or through the use of software that automates the process. If proper controls are not implemented to prevent this, a weakness could compromise CORNET data and applications.

An effective control to limit this exposure is to use a system-based control setting that will lock out a userid if a predetermined number of failed login attempts are made. Legitimate users whose login access is blocked need to re-authenticate themselves before system administrators will reopen access.

In this section, we looked at the controls in place to ensure that:

- all unsuccessful login attempts are recorded, reviewed and followed up if necessary.

Key Findings

- CORNET database accounts are automatically locked by the system after a pre-set number of failed login attempts.

We had no detailed recommendations in this area.

A5. Logical access to the database via database privileges

Staff who support and maintain the database need direct database access in varying degrees to perform their jobs. Often these access levels are very high, in some cases giving individuals the right to view all data in the database and the ability to create, edit, delete or copy and download data records. It is therefore imperative that this type of access be well controlled.

In this section, we looked at the controls in place to ensure that:

- all system and process database accounts are valid and authorized;
- database userids, roles and privileges are properly managed; and
- system privileges that could affect the operation of processes or the security of the database system are appropriately restricted and controlled.

Key Findings

- Three IT support groups share userids. The activities performed under these userids cannot be traced back to individuals. This creates a risk of unauthorized changes being made and no way of knowing who made them. All other users are issued their own unique userid, allowing for individual monitoring of users and an audit trail.
- Some key support staff have full access to the CORNET data, including the ability to alter the audit trail. For these users, insufficient monitoring is performed to compensate for this high risk activity.
- Powerful privileges that could affect the operation of processes or the security of the database system are, for the most part, secured and restricted to IT support staff.

We made 20 detailed recommendations in this area to improve logical database access.

A6. Logical access directly to the database via too

Most CORNET users obtain v
database through the access the
Behind the scenes, further authe
database management system t
accordance with their unique ac
circumstances, all users should
and not directly through the da

The risk of direct database ac
to download, view or alter data
through the application. Restric
database logins are important c

Another entry method to the
These are one-way access paths
from CORNET or imported fro
The activity associated with lin
ensure there is no unusual activ

In this section, we looked at

- users are appropriately r
the database;
- database links are secure
- the production database
non-production server.

Key Findings

- No monitoring is done t
users connecting directly
collected to determine w
the database.
- Database links are set up
to copy data from CORN
certain expected activity,
that the link is used appr
- A copy of the CORNET p
a test environment serve
maintenance, but in this
users could connect from

test server to the CORNET production database. The risk is that users might think they are using a test system and enter test data into the production database in error, inadvertently creating false records or modifying real CORNET records.

We made 11 detailed recommendations in this area to improve logical database access.

A7. Auditing at the database level

One of the most effective ways to monitor access is through the use of system-based audit logs. The logs, if properly set up and regularly monitored, can help identify unusual access patterns and indicate where there has been inappropriate access. To allow for effective monitoring, relevant and sufficient log information must be collected and retained. This is especially important for monitoring the activities of key support staff who have higher levels of database access rights.

Audit logs are available for the CORNET application as well as the Oracle database management system.

In this section, we looked at the controls in place to ensure that:

- audit trails are set up and recorded according to business risks;
- adequate monitoring tools are available to assist staff in analyzing the audit logs; and
- audit logs are secured, effectively record user activity, and are retained for monitoring.

Key Findings

- The CORNET audit logs adequately record all changes made to CORNET data, including the name of the user, date of change, and changes made to the data. These logs are never deleted, allowing monitoring to be done at any time. One concern, however, is that certain IT support users are able to alter these logs. (This was discussed in more detail in the findings for audit scope area A5, Logical access to the database via database privileges.)
- Standard Oracle database audit logs record information on where users are logged in from, as well as the date and time. These audit logs offer several potential uses, from identifying

inappropriate accesses made directly to the database and tracking database link activity to monitoring connections made from non-application servers to the production database. At present, however, these audit logs are not monitored and are kept for only 30 days.

We made seven detailed recommendations in this area to improve auditing at the database level.

A8. Logical access to the data via the application

Users are granted access to CORNET based on their job titles, facility location and application training completed. The access levels assigned restrict users to specific system modules (functions) and specific data records. Access assignment errors that go undetected could result in users having access to view, change, delete, or copy and download data they should not have access rights for. To detect anomalies in access assignments, monitoring needs to be done regularly.

Authority for external users (such as federal correctional officers and provincial Crown counsels) to access CORNET is governed through the use of electronic access agreements.

In this section, we looked at the controls in place to ensure that:

- access is defined in security matrices;
- module assignment to access groups is correct;
- access groups are assigned to users correctly, based on job function;
- location access is appropriately assigned to users;
- access to sensitive information, such as youth and sealed data, is properly controlled; and
- access agreements are in place for all external users and access has been set up accordingly.

Key Findings

- Security matrices define how access should be set in any system. For CORNET, these matrices do not exist for some positions and for others they are not kept up-to-date.
- Almost all (97%) of the time, employees are given the correct application access to view or change data, and the correct

location access based on their job functions. However, during our audit, we found incorrect accesses for about 100 users, which could allow the inappropriate viewing of some youth or sealed records.

- The computer program itself properly protects youth and sealed data when entry is through the application. But when entry is through the database (which should be limited to IT support staff and a few authorized users), there are no controls limiting access to youth and sealed data.
- Access for external users is based on agreements that clearly specify the business reasons for accessing CORNET.

We made 11 detailed recommendations in this area to improve logical database access via the application.

A9. Auditing at the application level

All users of the CORNET system have access to view or change some type of confidential data. Some are able to view or change all data in the database, while others have very restricted access. As with any situation of trust, when users are able to access data, there is always a remote possibility that they could abuse this trust. Depending on the type of data and the consequences that could result from its misuse, some level of effective auditing or monitoring must always be in place.

CORNET has the ability to report on all database changes made by specific users and on all changes made to specific offenders. It can also report specifically on sentence information, showing changes made to records by users and the associated authority documents, conditions, charge counts and sentences for a particular offender.

As well, CORNET has the ability to report on user activities initiated through certain application modules, and the audit capability to identify who looked at or changed particular data fields and when.

Special investigations requiring audit reports can also be run, but initiated only by provincial government directors. The ability to run these reports should only be accessible to the authorized support staff in the Ministry of Public Safety and Solicitor General.

In this section, we looked at the controls in place to ensure that:

- adequate audit reporting capabilities exist to allow for analysis of sensitive data.

Key Findings

- CORNET has the capability to report on all database changes made by specific users and on changes made for specific offenders, as well as the capability to identify who viewed particular data fields. This audit capability is sufficient and appropriately restricted to authorized staff.

We did not have any detailed recommendations in this area.

A10. Logical access to data via the host operating system

The CORNET database and application runs on the UNIX operating system, which is supported by Workplace Technology Services. If not properly set up, the operating system could provide unauthorized users or intruders a way into the database. Access to log into UNIX is controlled through userids and passwords, which must be properly secured and administered to prevent the risk of compromise. Access groups and privileges in UNIX must also be appropriate to reduce the risk of unauthorized access.

The number of staff with a need to access UNIX should be minimal. Only key support staff from Workplace Technology Services and the Ministry of Attorney General need UNIX userids. For those users, full access to view and change data in the CORNET database through the UNIX operating system is possible. Strong monitoring should be in place to ensure that any access made this way is legitimate—and to detect any unauthorized access.

In this section, we looked at the controls in place to ensure that:

- all userids that are able to log in to the host operating system (UNIX) represent valid, current users and are in the appropriate access groups;
- all user accounts have a password and there is a process to periodically change passwords;
- database files and logs are appropriately secured; and
- only authorized system administration personnel and processes are able to access the Oracle database owner userid.

Key Findings

- Access to the UNIX operating system is limited to a few Workplace Technology Services and Attorney General support staff. The UNIX privileges required by the Workplace Technology Services staff give them full access to the CORNET database, yet there is insufficient monitoring to track their activities.
- The password for the Oracle userid is set to the same value on all Attorney General database servers. If the password was compromised in any of the environments, it could potentially allow unauthorized access to all of the Attorney General's databases, not just CORNET. Appropriate safeguards are not in place to ensure security for this userid, nor is monitoring in place to allow unauthorized use to be detected.

We made 12 detailed recommendations in this area to improve logical database access.

A11. Logical access to the database via the network

Virtually all government offices use government's SPAN/BC network to communicate with the CORNET database and application servers. Before they can get access to log in to the system, they must pass through the firewall maintained by the Ministry of Attorney General. This firewall allows only certain networks and subnets[4] to get through to the Attorney General's servers that house the CORNET system. Users connecting from their homes or from remote sites not on SPAN/BC could gain access using other approved connection methods, such as SPAN/VPN, SecureClient, Nortel/VPN or DTS.

When data is transmitted on SPAN/BC or other approved external network, between workstations and the CORNET servers, it is safer to send it encrypted rather than in plain text. This way, if any hackers using special software tried to view and copy the data as it travelled through the network, they would not be able to read anything. However, if plain text transmissions are sent, then userids and passwords could also be compromised and used to gain unauthorized entry to the system.

[4] A subnet is part of a network that is usually assigned to a specific area. For example, each correction centre could be assigned its own subnet.

The Oracle "Listener" is a computer program that sets up connections between user workstations or servers and the database. It must be properly password-protected to reduce the risk of the program being disrupted, which could in turn stop the CORNET system.

In this section, we looked at the controls in place to ensure that:

- the Oracle Listener is properly secured;
- encryption is used between workstations, database servers and application servers; and
- the firewall settings allow only authorized networks, subnets and users employing approved connection methods through to the database and application servers housing the CORNET system.

Key Findings

- Data transfers between workstations and the CORNET application or database server are not adequately protected from exposure during transmission.
- The firewall settings are properly configured to prevent Internet traffic from passing through to the Attorney General's servers. Unauthorized access attempts to the CORNET database through the firewall are continually monitored by a contractor using intrusion detection software.
- The complexity in the design of the firewall settings increases the difficulty of managing it and could lead to incorrect access.
- There is excessive access through the firewalls to the servers housing the CORNET database, via access specifically granted to networks and through other approved connectivity methods mentioned above.
- Some users are able to access the CORNET system using connectivity software loaded on their personal home computers. If these users do not keep their computers protected with up-to-date anti-virus software, there is a risk that userids and passwords could be compromised through malicious software surreptitiously loaded and activated on their hard drives.

We made 13 detailed recommendations in this area to improve logical database access.

Organization-wide IT Security

Although the scope of our audit did not include assessing the overall governance of CORNET, we did have a finding related to the security group's effectiveness in promoting a more secure system.

Last year, a Justice Sector Information Security Framework was approved. It spells out the overall security framework for the justice sector, including business needs, overarching security principles, and the roles and responsibilities of those charged with governance. In terms of governance, the framework emphasizes the need for communications among all personnel involved in ensuring that a secure system is maintained.

In this section, we looked at the controls in place to ensure that:

- the security group structure is effective in promoting security in systems.

Key Findings

- There is insufficient involvement by the security group in some of the decisions made in the production environment that affect overall system security. An integrated approach is needed to ensure that an organization-wide approach to system security is carried out.

We made one detailed recommendation in this area to improve organization-wide security.

Patch Maintenance and Backup

Vendors' software very often contains known security vulnerabilities that are not identified until after the software is released. This is no different for the Oracle database, Oracle application server, or Solaris (UNIX) operating system. Vendors respond to known vulnerabilities by periodically sending out software upgrades (called patches) for clients to apply. It is up to the organization to determine how often to apply patches, if at all. Although doing so regularly can be time consuming, there is a risk in leaving systems without the most up-to-date protection from outside threats.

In this section, we looked at the controls in place to ensure that:

- patches are kept current; and
- procedures exist for creating back-ups of the database.

Key Findings

- Regular patching of security-related vulnerabilities, identified in the Oracle database, Oracle application server and UNIX operating system, is not done, leaving the systems at risk of being compromised. Mitigating strategies, such as the use of firewalls and intrusion detection software, can reduce this risk, but risks remain from other possible vulnerabilities.
- Automatic scheduling is in place for backing up the database at set times.

We made one detailed recommendation in this area to improve system maintenance.

Appendices

Appendix A: Office of the Auditor General Reports Issued Fiscal 2007/2008

Report 1 – April 2007
Special Audit Report to the Speaker: The Financial Framework Supporting the Legislative Assembly

Report 2 – June 2007
The Child and Youth Mental Health Plan: A Promising Start to Meeting an Urgent Need

Report 3 – October 2007
A Review of the Vancouver Convention Centre Expansion Project: Governance and Risk Management

Report 4 – December 2007
Follow-up of 2004/2005 Report 3: Preventing and Managing Diabetes in British Columbia

Report 5 – January 2008
Preventing Fatalities and Serious Injuries in B.C. Forests: Progress Needed

Report 6 – February 2008
Literacy: Creating the Conditions for Reading and Writing Success

Report 7 – March 2008
Improving Financial Reporting for British Columbians: Report on the 2006/07 Public Accounts

Report 8 – March 2008
Managing Access to the Corrections Case Management System

This report and others are available on our website at: http://www.bcauditor.com.